Running head: MAPPING CRITICAL INFRASTRUCTURE

Mapping Critical Infrastructure and Key Resources for the City of Irving

Scott A. Johnson Sr.

Irving Fire Department, Irving, Texas

Certification Statement

I hereby certify that this paper constitutes my own product, that where language of others is set forth, quotation marks so indicate, and that appropriate credit is given where I have used the language, ideas, expressions, or writings of another.

Signed:_____

Abstract

Homeland Security Presidential Directive – 7 established a national policy compelling federal departments and agencies to identify and prioritize critical infrastructure and key resources (CIKR) in the United States and to protect them from all hazards. Since 85% of all CIKR is owned and operated by entities other than the federal government, public/private partnerships were created to complete the task of identifying and mapping CIKR for use by the full spectrum of CIKR partners.

The problem was the City of Irving, Texas did not have a map of CIKR that could be used by fire department incident commanders in the field. The purpose of this research was to identify CIKR within the City of Irving, to database the findings, and to develop a portable map containing those CIKR locations. This applied research project used an action research method to answer the questions: What CIKR existed within the City of Irving and where was it located?

These questions were answered using Irving Fire Department Quick Action Plans, discussions with the Irving Department of Emergency Management, and extensive internet research. Once CIKR was identified, the locations were plotted on a virtual globe using Google Earth™. The data was organized alphabetically into the 18 CIKR sectors defined in the National Infrastructure Protection Plan and resulted in 771 individual CIKR locations being included in the first edition of the City of Irving CIKR Database and Map set.

Future editions of the database should expand the scope of data collection and include emergency contact information, digital floor plans, building system locations, building system operating instructions, and digital images of the location.

Additionally, DHS Earth and the Integrated Common Analytical Viewer should be evaluated as an alternative to developing a proprietary database and mapping system. Both of these applications were available through the Homeland Security Information Network.

Table of Contents

Introduction

In response to the September 11, 2001 World Trade Center attacks and the resulting crash of economic and financial structures in the United States, on December 17, 2003 President George W. Bush issued Homeland Security Presidential Directive/HSPD-7 (HSPD-7). This presidential directive established a national policy compelling federal departments and agencies to identify and prioritize critical infrastructure and key resources (CIKR) in the United States and to protect them from terrorist attacks (Bush, 2003). Shortly after this presidential directive was issued, the record setting 2005 Atlantic hurricane season battered the Gulf Coast of the United States. The Undersecretary of Commerce for Oceans and Atmosphere at the National Oceanic and Atmospheric Administration (NOAA), retired Vice Admiral Conrad C. Lautenbacher, characterized the 2005 Atlantic hurricane season by saying, “Arguably, it was the most devastating hurricane season the country has experienced in modern times” (National Oceanic and Atmospheric Administration, 2006). The resulting devastation from this hurricane season prompted the addition of natural disasters in federal policy relating to the protection of CIKR in the United States.

In section 8 of HSPD-7 President Bush (2003) states:

> Federal departments and agencies will identify, prioritize, and coordinate the protection of critical infrastructure and key resources in order to prevent, deter, and mitigate the effects of deliberate efforts to destroy, incapacitate, or exploit them. Federal departments and agencies will work with State and local governments and the private sector to accomplish this objective. (p.2)

Section 8 of HSPD-7 mandates the protection of CIKR within the United States. This section of the presidential directive also compels the cooperation of federal, state, and local governments in identifying and prioritizing CIKR within their respective jurisdictions. The problem is the City of Irving, Texas does not have a map of CIKR that can be used by fire department incident commanders in the event of an emergency within our jurisdiction.

The purpose of this research is to identify CIKR within the City of Irving, to database the findings of this research, and to develop a portable map indicating the locations of the CIKR contained in the database. This applied research project will use an action research method and answer the following research questions: (a) What critical infrastructure exists within the City of Irving, (b) What key resources exist within the City of Irving, and (c) Where are the CIKR located within the City of Irving?

Background and Significance

The 9/11 Attacks

On September 11, 2001 four commercial passenger jets were hijacked by 19 al-Queda terrorists. Two of these jets were crashed into the twin towers of the World Trade Center in New York City. The third jet was crashed into the Pentagon in Washington, D.C. and the fourth jet was crashed into a field near Shanksville, Pennsylvania when the passengers and crew attempted to retake control of the plane. This fourth plane had been redirected toward Washington, D.C. and was targeting either the Capitol Building or the White House (The 9/11 Commission, 2004).

With death tolls in the thousands and the collapse of these iconic buildings came the collapse of the American illusion that we were safe at home and could not be attacked on

U.S. soil. This insecurity in the American psyche led to the collapse of long standing economic and financial institutions and highlighted their dependency on the CIKR that undergirded their emotional, physical, and economic stability.

Homeland Security Presidential Directive/HSPD-7

On December 17, 2003, President George W. Bush issued HSPD-7. The purpose of this presidential directive was to establish a national policy for identifying CIKR, prioritizing their importance, and planning protective measures against terrorist attacks. In this directive, federal departments and agencies were tasked to coordinate with state and local governments and with the private sector to accomplish this task (Bush, 2003).

The 2005 Atlantic Hurricane Season

The 2005 Atlantic hurricane season was the most active ever recorded. Of the 31 named storms, hurricanes Katrina and Rita garnered the most attention as they battered the Gulf Coast and twice flooded the City of New Orleans, Louisiana. Hurricane Katrina, which made landfall on August 29, 2005, was one of the deadliest storms in generations with 1833 fatalities and an estimated $81 billion in total damages. With a 30 foot storm, the levies protecting the City of New Orleans broke and caused wide spread flooding (Knabb, Rhome, & Brown, Tropical cyclone report - Hurricane katrina - 23 to 30 august 2005, 2006). While still assessing the aftermath of Katrina’s devastation, Hurricane Rita made landfall on September 24, 2005. With a storm surge of 15 feet, flooding in Louisiana occurred in the City of Lake Charles, the Parishes of Vermillion, Iberia, St. Mary, and again in the City of New Orleans. Hurricane Rita provoked one of the largest evacuations in U. S. history with an estimated 2 million people being evacuated in Texas alone. Hurricane Rita is cited with 55 fatalities and $10 billion in property damage

(Knabb, Brown, & Rhome, Tropical Cyclone report - Hurricane rita - 18 to 26 september 2005, 2006). Some of the critical infrastructure affected by these storms included oil platforms, pipelines, and refineries; water mains; electric power lines; and cellular telephone towers. In some instances, key resources such as the City of New Orleans police and fire departments were rendered incapable of providing service to their community. The loss of this CIKR caused a disruption in the functioning of local governments and business and produced cascading effects that reached national proportions (United States Government Accountability Office, 2006). The devastation these hurricanes caused to CIKR along the gulf coast prompted natural disasters to be added to the list of things that CIKR should be protected against.

All Government is Local

While federal departments and agencies have been mandated to coordinate the identification and protection of CIKR, state and local governments, along with the private sector, own and operate 85% of the CIKR within the Unites States. In order for a complete CIKR inventory to be conducted, each state and local government jurisdiction or private sector entity must be involved in the process (United States Government Accountability Office, 2006).

Once a CIKR inventory has been completed, the information must be compiled into a database and made available to decision makers for prioritizing their importance and coordinating their protection. In the event of a disaster, of either human or natural origin, this information must be made available to decision makers in the Emergency Operations Center (EOC). While the CIKR database provides valuable information to public and private sector decision makers operating in the EOC, experience in the EOC Simulation

Labratory during the National Fire Academy course *Executive Analysis of Fire Service Operations in Emergency Management* has proven that a map with all of the CIKR information displayed provides a priceless graphical tool for in-depth situational analysis and supplies a vehicle for disseminating a common operating picture.

The development of a CIKR database and a CIKR map not only prepares public and private decision makers for catastrophic possibilities, for the state and local fire service entities involved, it moves them closer to attaining the first four goals in the strategic plan of the United States Fire Administration by: reducing the risk at the local level through prevention and mitigation; improving local planning and preparedness; improving the fire and emergency services' capability for response to, and recovery from, all hazards; and improving the fire and emergency services' professional status

Literature Review

Homeland Security Presidential Directive/HSPD-7

Issued on December 17, 2003 by President George W. Bush, HSPD-7 is the seminal document driving all efforts toward critical infrastructure identification, prioritization, and protection. The stated purpose of this directive is to establish "a national policy for Federal departments and agencies to identify and prioritize United States critical infrastructure and key resources and to protect them from terrorist attacks" (Bush, 2003, p. 1) .

In the Background section of HSPD-7 president Bush (2003) states:

> (2) Terrorists seek to destroy, incapacitate, or exploit critical infrastructure and key resources across the United States to threaten national security,

cause mass casualties, weaken our economy, and damage public morale and confidence.

(3) America's open and technologically complex society includes a wide array of critical infrastructure and key resources that are potential terrorist targets. The majority of these are owned and operated by the private sector and State or local governments. These critical infrastructures and key resources are both physical and cyber-based and span all sectors of the economy.

(4) Critical infrastructure and key resources provide the essential services that underpin American society. The Nation possesses numerous key resources, whose exploitation or destruction by terrorists could cause catastrophic health effects or mass casualties comparable to those from the use of weapons of mass destruction, or could profoundly affect our national prestige and morale. In addition, there is critical infrastructure so vital that its incapacitation, exploitation, or destruction, through terrorist attack, could have a debilitating effect on security and economic well-being.

(5) While it is not possible to protect or eliminate the vulnerability of all critical infrastructure and key resources throughout the country, strategic improvements in security can make it more difficult for attacks to succeed and can lessen the impact of attacks that may occur. In addition to strategic security enhancements, tactical security improvements can be rapidly implemented to deter, mitigate, or neutralize potential attacks (p. 1).

In the Policy section of HSPD-7, subsection 8, federal departments and agencies are mandated to “identify, prioritize, and coordinate the protection of critical infrastructure and key resources” in order to “prevent, deter, and mitigate the effects of deliberate efforts to destroy, incapacitate, or exploit them”, and to “work with State and local governments and the private sector to accomplish this objective” (Bush, 2003, p. 2).

In the Roles and Responsibilities of the Secretary section of HSPD-7, subsection 15, the Secretary of Homeland Security is charged with the coordination of protection activities for 6 critical infrastructure sectors. These sectors include: information technology; telecommunications; chemical; transportation systems, including mass transit, aviation, maritime, ground/surface, and rail and pipeline systems; emergency services; and postal and shipping. The Department of Homeland Security (DHS) is also charged with coordinating the protection of other key resources including dams, government facilities, and commercial facilities (Bush, 2003).

The National Plan for Research and Development in Support of Critical Infrastructure Protection.

The 2004 *National Plan for Research and Development in Support of Critical Infrastructure Protection* plan document was the first annual version of the research and development roadmap for critical infrastructure protection. This document was released on April 8, 2005 and focused on “the identification of capabilities, needs, and gaps based on known threats. With this baseline in place, a roadmap and investment plan can be developed for the 2005 national critical infrastructure protection research and development planning effort” (The Department of Homeland Security Science and Technology Directorate, 2005, p. iiv).

The National Critical Infrastructure Protection Research and Development (NCIP R&D) Plan addresses the physical, cyber, and human elements of the critical infrastructure sectors. The plan is structured around nine science, engineering, and technology themes that support all of the critical infrastructure sectors. These nine themes include: “detection and sensor systems; protection and prevention; entry and access portals; insider threats; analysis and decision support systems; response, recovery, and reconstitution; new and emerging threats and vulnerabilities; advanced infrastructure architectures and systems design; and human and social issues” (The Department of Homeland Security Science and Technology Directorate, 2005, p. vii). The plan is also driven by three strategic goals: “A national common operating picture for critical infrastructure”, “A next generation computing and communications network with security ‘designed-in’ and inherent in all elements rather than added after the fact”, and “Resilient, self-diagnosing, and self-healing physical and cyber infrastructure systems” (The Department of Homeland Security Science and Technology Directorate, 2005, p. viii).

The NCIP R&D Plan (2004) acknowledges that CIKR protection cannot be accomplished by the federal government alone but must be a coordinated effort of the federal government, state governments, local governments, the private sector, and private citizens from across the country. It also makes clear that critical infrastructure is not limited to buildings and structures but also includes the people, physical systems, and cyber systems that work interdependently to make the wheels of commerce and government continue to turn. Some of the key nodes of commerce and government that constitute critical infrastructure are identified as industrial complexes, airports, control

and communication centers, power plants, locks and dams, and farms. Also seen as critical infrastructure are the indispensable interconnecting links such as transportation systems, utilities, and the internet that are essential to the continued functioning of commerce and government (p. 2).

The NCIP R&D Plan (2004) expounded on the critical infrastructure sectors and key resources laid out in HSPD-7 and identified these 17 assets deemed critical to the nation: agriculture and food; water; public health and healthcare; emergency services; defense industrial base; information technology; telecommunications; energy; transportation systems; banking and finance; chemical; postal and shipping; national monuments and icons; dams; government facilities; commercial facilities; and nuclear reactors, materials, and waste (p.3).

After identifying the assets that are deemed critical to the nation, the NCIP R&D Plan (2004) changed the standing practice of organizing CIKR by sectors and began the practice of organizing CIKR by themes. The reasoning for this change was based in five common traits that challenged sectoring's ability to efficiently and effectively address areas such as research and development. The first of these traits was that several sectors contained infrastructure that were vulnerable to exactly the same threats. The use of a sector based approach created repetition and a loss of opportunity for integration. The second trait was that sectoring did not address the inherent interconnectedness and interdependence between sectors. The third trait was the tendency to separate the consideration of cyber systems and physical systems. The themed system would address these systems in an integrated and interdependent manner. The fourth trait was the separation between efforts to reduce vulnerability in existing infrastructure and efforts to

design new infrastructure for higher performance and quality of service. The fifth trait was the challenge of evaluating new threats and opportunities from new technological advances that cut across sectors and were not analyzed by more specialized systems designers (p. 4).

The NCIP R&D Plan (2004) then defines these nine themes and gives an example of a key future capability that must be accomplished to make progress toward the stated long term strategic goals:

> **THEME 1:** Detection and Sensor Systems – Detection and sensor systems and related integration needs.
>
> FUTURE CAPABILITY: Systems and tools to detect and sense what is occurring or anticipate actions.
>
> **THEME 2**: Protection and Prevention – Protection of assets and prevention of successful attacks against them.
>
> FUTURE CAPABILITY: Systems, tools, methods, and permissions to protect assets and connections critical to the nation.
>
> **THEME 3**: Entry and Access Portals.
>
> FUTURE CAPABILITY: Prevent unauthorized access to important places and systems.
>
> **THEME 4**: Insider Threats.
>
> FUTURE CAPABILITY: Protect systems against a trusted party who has passed all controls, is inside key assets, and proceeds to do harm.
>
> **THEME 5**: Analysis and Decision Support Systems.

FUTURE CAPABILITY: Tools that can analyze complex and difficult problems and support decision making in the most integrated and informed way possible.

THEME 6: Response, Recovery, and Reconstitution.

FUTURE CAPABILITY: Be prepared to manage a critical event situation from initial response to final replacement of the lost asset or capability.

THEME 7: New and Emerging Threats and Vulnerabilities.

FUTURE CAPABILITY: Develop the tools, methods, and technologies to discover at the earliest possible time that an adversary can now deliver a new threat.

THEME 8: Advanced Infrastructure Architecture and System Design.

FUTURE CAPABILITY: Build new systems that do not have the faults or limitations of past systems and technologies that were created at a time when security was not a driving issue.

THEME 9: Human and Social Issues.

FUTURE CAPABILITY: New user interfaces that accept, organize, and present unprecedented quantities of information in a form that enables much faster understanding and more accurate decision making in crisis (p. 15).

Critical Infrastructure Protection – Progress Coordinating Government and Private Sectors Efforts Varies by Sectors' Characteristics

The report *Critical Infrastructure Protection – Progress Coordinating Government and Private Sectors Efforts Varies by Sectors' Characteristics* was published on October 16, 2006 by the United States Government Accountability Office (GAO). In this report, hurricane Katrina is cited as the cause of critical infrastructure damage along the Gulf Coast and prompted the inclusion of natural disasters in the list of threats that CIKR should be guarded against. Also included in this report is an acknowledgement that the private sector owns 85% of the nation's critical infrastructure necessitating the need for the "public and private sector to form effective partnerships to successfully protect these assets" (United States Government Accountability Office, 2006, p. 1).

Interestingly, this report does not mention the nine themes defined in the 2004 NCIP R&D Plan. Instead, there is a return to the use of sectors with an individual sector being assigned to each of the 17 assets deemed critical to the nation in the 2004 NCIP R&D Plan. For each of the 17 sectors, sector specific federal agencies are commissioned with infrastructure protection activities in their assigned sectors. Included in this commission is "coordinating and collaborating with relevant federal agencies, state and local governments, and the private sector to carry out sector specific responsibilities." Also included in this commission was "facilitating the sharing of information about physical and cyber threats, vulnerabilities, incidents, potential protective measures, and best practices." These sector specific agencies (SSA's) are required to "submit an annual report to the DHS on their efforts to identify, prioritize, and coordinate the protection of critical infrastructure in their respective sectors" (United States Government Accountability Office, 2006, p. 11).

The federal agencies responsible for the first seven sectors are: Agriculture and Food – Department of Agriculture, Department of Health and Human Services, and the Food and Drug Administration; Defense Industrial Base – Department of Defense; Energy – Department of Energy; Public Health and Healthcare – Department of Health and Human Services; National Monuments and Icons – Department of Interior; Banking and Finance – Department of Treasury; Drinking Water and Water Treatment Systems – Environmental Protection Agency. The remaining 10 sectors are the responsibility of the DHS. The DHS Office of Infrastructure Protection is responsible for the following sectors: Chemical; Commercial Facilities; Dams; Emergency Services; Commercial Nuclear Reactors, Materials, and Waste. The DHS Office of Cyber Security and Telecommunications is responsible for the Information Technology sector and the Telecommunications sector. The DHS Transportation Security Administration is responsible for the Postal and Shipping sector. The DHS Transportation Security Administration and United States Coast Guard are responsible for the Transportation Systems sector and the DHS Immigrations and Customs Enforcement and Federal Protective Service are responsible for the Government Facilities sector (United States Government Accountability Office, 2006).

For each of these sectors, the National Infrastructure Protection Plan (NIPP) Partnership Model "requires the formation of government coordinating councils (government councils) – comprised of federal, state, local, or tribal agencies with purview over critical assets." The NIPP Partnership Model also "encourages voluntary formation of sector coordinating councils (sector councils) – comprised of owner-operators of these critical assets (some of which may be state or local agencies) or their

respective trade associations." The purpose of these government and sector councils is to create a representative structure "from all levels of government and the private sector to collaborate in planning and implementing efforts to protect critical infrastructure." The sector councils are intended to be policy related and designed to be a primary point of contact for the federal government "to plan the entire range of infrastructure protection activities unique to that sector" (United States Government Accountability Office, 2006, p. 3).

In attempting to form government and sector councils, council representatives identified these three major challenges that hampered their progress:

> 1) Difficulties establishing partnerships with the DHS because of issues with high turnover of its staff and DHS staff who lacked knowledge about the sector to which they were assigned; 2) Hesitancy to provide sensitive information or industry vulnerabilities to the government due to concerns that the information might be publicly disclosed; and 3) Lack of long-standing working relationships within the sector or with federal agencies (United States Government Accountability Office, 2006, p. 20).

Of these challenges, hesitancy to provide sensitive information to the government remains the most difficult to overcome. Representatives for about a third of the councils, six government councils and five sector councils, noted that the private sector continues to be hesitant to provide sensitive information due to concern that it might be publicly disclosed. The specific concern was that information discussed may be subject to public disclosure under the Federal Advisory Committee Act making this information "available to competitors or potentially make the council members subject to litigation for failure to

publicly disclose any known threats or vulnerabilities" (United States Government Accountability Office, 2006, p. 26). In researching this concern, the GAO assessed the status of the DHS efforts to implement the Protected Critical Infrastructure Information (PCII) program. This program was implemented in anticipation of reluctance on the part of the private sector to provide sensitive information. The PCII program was "specifically designed to establish procedures for the receipt, care, and storage of critical infrastructure information voluntarily submitted to the government." The GAO found that the DHS had created the program office, provided a program structure, and had provided guidance in the use of the program. The GAO even found that a few private sector entities were using the program. However, the challenges faced by the DHS with respect to this program included not being able to assure the private sector that sensitive information would indeed be protected, specifying who would be authorized to have access to the information, and demonstrating any benefits of sharing the information to the owners of the critical infrastructure (United States Government Accountability Office, 2006, p. 27).

A Guide to Critical Infrastructure and Key Resource Protection at the State, Regional, Local, Tribal, and Territorial Level

A Guide to Critical Infrastructure and Key Resource Protection at the State, Regional, Local, Tribal, and Territorial Level was published by the DHS Office of Infrastructure Protection in September 2008. In the opening letter, Robert Stephan, Assistant Director of the Office of Infrastructure Protection describes this guide by saying:

> This document outlines the attributes, capabilities, needs, and processes that a State or other governmental entity should include in establishing its

> own CIKR protection function such that it integrates with the NIPP and accomplishes the desired local benefits. It is intended to serve as a "why-to" rather than a "How-to" guide. The guide is not intended to be prescriptive or impose requirements on the States, communities, or other CIKR partners. Rather, it suggests various strategies and approaches, and leaves it to the discretion of each State, region, or locality to determine which approach or combination of approaches, if any, might be suited to their specific needs, operating environments, and risk landscapes (Office of Infrastructure Protection, 2008).

The thesis of this document is that there may be CIKR that are very important on the state or local level that are not nationally significant. Because of these localized concerns, "it is important for State, regional, local, tribal, and territorial CIKR protection and resiliency efforts to help implement the NIPP and the associated Sector-Specific Plans (SSPs), and also to support more specific, localized concerns" (Office of Infrastructure Protection, 2008, p. 1).

The goal of the NIPP is to:

> Build a safer, more secure, more resilient America by enhancing protection of the Nation's critical infrastructure and key resources (CIKR) to prevent, deter, neutralize, or mitigate the effects of deliberate efforts by terrorists to destroy, incapacitate, or exploit them; and to strengthen national preparedness, timely response, and rapid recovery in the event of attack, natural disaster, or other emergency. (Office of Infrastructure Protection, 2008, p. 3)

Generally, the most visible and tangible efforts to provide CIKR protection in the eyes of the public, and CIKR owner/operators, are non-federal efforts implemented by a local form of government. From a jurisdictional perspective, non-federal CIKR protection programs support the NIPP by providing a jurisdictional focus, bottom up information sharing and collaboration, and enable cross-sector coordination by applying the NIPP risk management framework across the vertically organized CIKR sectors within their communities (Office of Infrastructure Protection, 2008). Again, bottom up information sharing and collaboration often causes hesitation on the part of local governmental entities. However, "the primary objective of the NIPP approach to information sharing is to enhance situational awareness and maximize the ability of government and private sector CIKR partners at all levels to assess risks and execute risk mitigation programs and activities" (Office of Infrastructure Protection, 2008, p. 4). If information sharing and protection is done according to NIPP information sharing protocols, information should only be disseminated on a need to know basis. According to the NIPP:

> Effective CIKR information sharing relies on the balance between making information available to the appropriate authorities at all levels of government and the ability to protect sensitive or proprietary information, the disclosure of which might compromise on going law enforcement, intelligence, or military operations or methods. Dissemination of that information is therefore based on an end-user's homeland security responsibilities and "need to know" the information in question. Whether the information is "top down" (by partners working with national-level information such as system-wide aggregate data or the results of emergent

> threat analysis by the Intelligence Community) or "bottom-up" (by field personnel or facility operators sharing detailed and location specific information), the network approach places shared responsibility on all CIKR partners to adhere to applicable information sharing protocols and practices (Office of Infrastructure Protection, 2008, p. 4).

With the information sharing protocols in place, state and local jurisdictional governments should implement the NIPP to the extent that their budget and resources will allow. "Most disruptions or malevolent acts that impact CIKR begin and end as local situations. Local authorities typically shoulder the weight of initial prevention, response, and recovery operations until coordinated support from other sources becomes available" (Office of Infrastructure Protection, 2008, p. 14). "Fundamentally, State and local organizations should implement their homeland security missions to ensure public safety and welfare and provide for continued delivery and operation of essential services to their constituencies" (Office of Infrastructure Protection, 2008, p. 10).

Critical Infrastructure Protection – Update to National Infrastructure Protection Plan Includes Increased Emphasis on Risk Management and Resilience

The NIPP was originally published in 2006 with planned revisions every three years. In January 2009, DHS released the first update to their initial effort at protecting the nation's infrastructure (United States Government Accountability Office, 2010). In the 2009 version of the NIPP, the DHS created an 18th critical infrastructure sector for Critical Manufacturing and removed the list of threats that CIKR are to be protected against replacing it with an increased emphasis on DHS's all hazards approach to CIKR protection and planning.

The most striking revision in this update is an increased emphasis on the resiliency of CIKR and not just on protection. Since the publication of the first edition of the NIPP, members of Congress, thinkers in the academic realm, and CIKR partners in the private sector have expressed concerns that DHS has placed too many eggs in the protection basket and has left the resiliency basket woefully neglected. In this debate, protection is defined as "actions to deter the threat, mitigate vulnerabilities, or minimize the consequences associated with an attack or disaster" and resiliency is defined as "the ability to resist, absorb, recover from, or successfully adapt to adversity or a change in conditions" (United States Government Accountability Office, 2010, p. 4). In its report, *Critical Infrastructure Resilience Final Report and Recommendations,* the National Infrastructure Advisory Council (2009) stated:

> The challenge facing government is to maintain its role in protecting critical infrastructure, while determining how best to encourage market forces to improve the resilience of companies, provide appropriate incentives and tools to help entire sectors become resilient, and step in when market forces alone cannot produce the level of infrastructure security needed to protect citizens, communities, and essential economic systems. (p. 10)

In the 2009 version of the NIPP, the DHS did not decrease its emphasis on the protection of CIKR. However, the DHS did increase its emphasis on resiliency by discussing it alongside of protection instead of treating it as a subset of protection. This is highlighted by noting the 2006 chapter titled *Characteristics of Effective Protection Programs* has been changed to *Characteristics of Effective Protection Programs and*

Resiliency Strategies in the 2009 version of the NIPP (United States Government Accountability Office, 2010).

How to Fix Critical Infrastructure Protection plans: A Guide for Congress

The report, *How to Fix Critical Infrastructure Protection Plans: A Guide for Congress* was published on April 27, 2010 in The Heritage Foundation publication *Backgrounder*. The fundamental themes in this report are: "Not all infrastructure is equally important, nor can every aspect be protected equally, so the focus must be on the protection of *critical* infrastructure"; "The NIPP lacks adequate tools to assess and manage risks in a way that accurately accommodates the complexity and dynamics of infrastructure, and the current system of congressional oversight is cumbersome and confusing"; and "Building solid relationships between the government and the private sector… and encouraging their investment in infrastructure quality can increase the likelihood that critical infrastructure can continue to function, or bounce back quickly, after a terrorist attack or natural disaster" (McNeill & Weitz, 2010, p. 1).

In their report, McNeill and Weitz (2010) lay out six reasons why they feel the current approach to critical infrastructure protection employed by the DHS and its partners is inadequate. They begin by citing the complexity and variety of CIKR that needs to be protected. McNeill and Weitz contend that the DHS "has failed repeatedly to recognize this fact – and continues to give infrastructure the same weight of risk and equal distribution of resources. In fact, not all infrastructure is at risk to terrorism or natural disasters." For this reason, they feel that a "National Risk Assessment is a bad idea. A National Risk Assessment simply does not make sense given the fact that the

varied levels of risk in today's infrastructure make it nearly impossible to create a standardized computation of risk" (p.4).

The second concern McNeill and Weitz (2010) have with the NIPP is its overuse of the term critical. They contend that policy makers lean on the critical designation because they are uncomfortable admitting that not all attacks and accidents can be prevented and even find an incentive to label infrastructure as critical because of the resources that become available with that designation. They contend:

> Addressing this challenge will require a shared effort between the private sector and the federal government, as well as hard choices, to disaggregate what is 'critical' (essential for supporting and sustaining American's daily lives) from what is 'dangerous' (e.g., chemical facilities) but not necessarily critical (p. 4).

The third concern McNeill and Weitz (2010) have with the NIPP is what they deem as lip service to the concept of resiliency. They state that "resiliency should not be used to indicate more across-the-board spending on infrastructure protection or more guns, gates, and guards." Their definition of resiliency "involves steps to increase the likelihood that critical infrastructure can continue to function or bounce back quickly despite a disruptive event" (p.4).

The fourth concern McNeill and Weitz (2010) have with the NIPP is the inadequacy of information sharing channels. They cite the concerns of the private sector about the legal and regulatory consequences of providing federal authorities with information concerning their sensitive and proprietary critical infrastructure activities.

McNeill and Weitz do not offer a solution to this concern but charge the federal government with mitigating the private sectors concerns in this area (p. 4).

The fifth concern McNeill and Weitz (2010) have with the NIPP is the lack of definition associated with the various CIKR partnerships described throughout the NIPP. They acknowledge "these public-private partnerships are essential to CIKR protection since the private sector owns and manages an estimated 85 percent of all critical infrastructure in the United States." However, they feel that these partnerships "need a better idea of the roles and responsibilities of both the private sector and the federal government – including vulnerability assessments, determining criticality, and other activities involving critical infrastructure protection" (p.5).

The final concern McNeill and Weitz (2010) state in this article concerns the agility of the federal government in the face of a very dynamic assessment of threats. Even the DHS stressed that the SSP's were not finished products but needed to be living documents that provide a general framework for future planning. However, in the view of McNeill and Weitz "part of changing in the face of new threats is developing an accurate picture of risk, and the NIPP is not agile enough to do so" (p. 5).

Homeland Security Information Network

To address the information sharing dilemma faced by the DHS, the Homeland Security Information Network (HSIN) has been developed. The HSIN is a secured web-based portal for information sharing and collaboration between CIKR partners on the federal, state, local, tribal, and territorial levels of government, as well as international CIKR partners and CIKR partners in the private sector. The HSIN is arranged into Communities of Interest (COI) that have been organized by state organizations, federal

organizations, or by mission areas with a critical interest in CIKR protection and resiliency. Some of these mission areas include emergency management, law enforcement, critical infrastructure sectors, and intelligence. The HSIN's secure web portal provides a suite of real-time collaboration tools that include a virtual meeting space, instant messaging, document sharing tools, the DHS Common Operational Picture (COP), the Automated Critical Asset Management System (ACAMS), the Integrated Common Analytical Viewer (iCAV), and DHS Earth. Membership in the HSIN is COI-based and new members are required to undergo a nominating and vetting process through the COI validating authority (United States Department of Homeland Security, 2011).

DHS Common Operational Picture

The DHS COP was created as a Post-Katrina After Action Report requirement. The use of this application allows HSIN users to "collect, capture, and publish graphic imagery. The COP application allows critical decision makers to define and prioritize the information they require for their operational activities, and display that data in manners that best facilitate their mission" (Phillips, 2007).

Automated Critical Asset Management System (ACAMS)

ACAMS is a secure web-based information services portal that assists state and local law enforcement, public safety entities, and emergency response personnel with collecting and using CIKR asset data, assessing CIKR asset vulnerabilities, developing all-hazard incident response and recovery plans, and building public-private partnerships. ACAMS can be used for "cataloguing, screening and sorting data; the production of tailored infrastructure reports; and the development of a variety of pre- and post-incident

response plans useful to strategic and operational planners and tactical commanders." This application provides state and local jurisdictions with a practical way to implement the NIPP using the NIPP Risk Management Framework and is provided at no cost by the DHS Office of Infrastructure Protection (United States Department of Homeland Security, 2009).

Integrated Common Analytical Viewer (iCAV)

iCAV "is a secure, web-based, geo-spatial visualization suite of tools that integrates commercial and government-owned data and imagery from multiple sources." The iCAV application resulted from the HSPD-7 mandate to "geospatially map, image, analyze, and sort the nation's critical infrastructure and key resources" and displays this information using a browser-based 2D viewer with 400 infrastructure layers, worldwide population data, real-time situational awareness data, and weather related information. iCAV also provides tools to "view the daytime verses nighttime ambient population distribution, inquire about the approximate population for an area, create polygons to depict areas of potential flooding as part of an inundation analysis, and visualize areas for rough chemical spill analysis." iCAV can be accessed by anyone with a HSIN username and password (United States Department of Homeland Security, 2010).

DHS Earth

"DHS Earth is a Keyhole Markup Language (KML) data feed that can be viewed using any geospatial visualization software compatible with KML files, such as Google Earth™ mapping service or Microsoft Virtual Earth." The DHS Earth data feed provides homeland security related data in a KML format, infrastructure data layers from the 18 CIKR sectors, and intuitive user interface, rapid response times, and 3D globe-based

viewers. DHS Earth can be accessed by anyone with an HSIN username and password (United States Department of Homeland Security, 2010).

Critical Infrastructure Protection – 9/11Plus Ten Years and Counting

When the twin towers of the World Trade Center came crashing down, the world as we knew it changed. The silo mentality of jurisdictional governments and the private sector would no longer be tenable in our new interdependent, interoperable, war on terror world. We need to learn new ways to function in local, regional, and national partnerships. From the perspective of CIKR protection, the NIPP provides a framework for protecting critical infrastructure and is well on its way to providing incentives for the private sector to engineer resiliency into newly designed infrastructure. The federal government cannot provide all of the solutions to CIKR protection and resiliency problems across all 18 critical infrastructure sectors. CIKR partners from across the spectrum will be required to rethink their roles in keeping America safe with our new all hazards mind set.

From the fire service perspective, we must see CIKR in our communities with new eyes and plan our responses with a new vision. The fire service is on the front lines in the war on terror. The fire service is also on the front lines in the event of natural disasters and man-made disasters. We must identify our resources before an actual event. We must also define our partnerships before an actual event and we must plan our responses accordingly. Using the National Response Framework, the NIPP, SSP's, and CIKR partners at the DHS, state level partners, local public safety partners, local government partners, and private sector partners we can develop plans and procedures to protect the CIKR that is valued by our constituents and build resiliency into our planning processes.

The effort to protect CIKR on a national, state, regional, and local level is an evolving process. It is a new frontier that has required exploration and experimentation. It has required trial and error and has moved forward with appreciable accomplishments but along the way has uncovered obstacles that have yet to be overcome. Only as we press forward in public and private sector CIKR partnerships will we work past our current concerns and begin to address CIKR concerns that have yet to be revealed.

Procedures

This research project was prompted by the lack of CIKR information available at emergency incident locations to Irving Fire Department Battalion Chiefs assigned to operations. These officers are the incident commanders charged with planning emergency operations in an all hazards environment. Their ability to understand the status of the situation, make wide-ranging tactical decisions, and develop a common operating picture for other fire ground decision makers has been severely disadvantaged by a deficiency in readily available geographical information.

Purpose of the Research

The purpose of this research was to identify CIKR within the City of Irving, to database the findings of this research, and to develop a map indicating the locations of the CIKR contained in the database. In order to realize these objectives, the following research questions were answered:

1. What critical infrastructure exists within the city of Irving?
2. What key resources exist within the City of Irving?
3. Where are the critical infrastructure and key resources located within the City of Irving?

Procedures for the Research

The literature review for this Applied Research Project began at the National Fire Academy's Learning Resource Center in December of 2010. This research included a search of Executive Fire Officer Program Applied Research Projects, trade publications, and journal articles pertaining to the topics of: CIKR, critical infrastructure, key resources, geographical information systems, GIS, interactive maps, online mapping, National Response Framework, National Infrastructure Protection Plan, and Homeland Security Infrastructure Protection.

Additional internet research was conducted, during multiple sessions, from December 2010 thru July 2011 using the Google and Yahoo search engines with search terms such as: CIKR, critical infrastructure, key resources, geographical information systems, GIS, interactive maps, online mapping, using Google maps, Google map icons, using Google Earth, Google Earth icons, ESRI, NAVTEQ, PLATTS, pipeline maps, City of Irving, Irving Independent School District, Carrollton Farmers Branch Independent School District, Coppell Independent School District, hotels, banks, church, electrical distribution systems in Irving, TX., TXU, Oncor, Atmos Energy, natural gas pipeline maps, refined petroleum pipeline maps, college, university, private school, hospital, emergency care clinic, veterinarian, United States Post Office, FedEx, UPS, trucking, shipping, freight, DFW Airport, Dallas Area Rapid Transit, DART rail, Trinity Rail Express, rail freight, water distribution systems in Irving, TX., and water treatment plant.

Significant Terminology

Answering the first research question required defining the term *critical infrastructure*. Critical infrastructure was defined as:

> Systems and assets, whether physical or virtual, so vital to the United States that their incapacity or destruction would have a debilitating impact on national security, national economic security, national public health or safety, or any combination of those matters (United States Government Accountability Office, 2007, p. 1).

This definition denotes a national significance that may not be applicable from the local perspective. To make it more locally relevant, the definition of critical infrastructure was changed to: Systems and assets, whether physical or virtual, so vital to the City of Irving that their incapacity or destruction would have a debilitating impact on local security, local economic security, local public health or safety, or any combination of those matters.

Answering the second research question required defining the term *key resources*. Key resources was defined as: "Publically or privately controlled resources essential to minimal operations of the economy or government, including individual targets whose destruction would not endanger vital systems but could create a local disaster or profoundly damage the nation's morale or confidence" (United States Government Accountability Office, 2007, p. 1).

This definition also denotes a national significance that may not be applicable from the local perspective. To make it more locally relevant, the definition of key resources was changed to: Publically or privately controlled resources essential to minimal operations of the local economy or local government, including individual targets whose destruction could create a local disaster.

These definitions were useful until an attempt was made to categorize each of the CIKR locations as either a critical infrastructure location or as a key resource location. At this point, the lines blurred and a majority of the locations found could be placed in either, or both, categories depending on the situation at hand in our new all hazards environment.

A Starter Map

On February 23, 2011, Billy Owens, an Emergency Management Planner with the City of Irving Department of Emergency Management was consulted about any CIKR maps that had already been developed for the City of Irving. He provided a digital copy of a map with 70 schools, 113 local government facilities, city limit boundaries, and the boundaries for D/FW Airport (see Appendix A). This map had been printed in an eight foot by five foot large format, laminated, and mounted on the wall of the Emergency Operations Center (W. Owens, personal communication, February 23, 2011).

This map provided a starting point but the size of the map and its physical nature prevented it from being useful in the back of an incident commanders suburban. This map would also be difficult to update as CIKR were added to the database. To meet the requirements of portability and the capability to update the CIKR database, the information from the City of Irving Department of Emergency Management CIKR map was transferred to a Google map.

Google Map

Google maps are a user-friendly mapping technology that features dragable maps, satellite imagery, and street view imagery with the capability to save an unlimited number of locations identified by icons, names, and descriptions (Google, 2011). To

establish a permanent residence for the map an email account was established using Google's free email system, Gmail. Once the email address was established, it was used to sign into Google maps. Once in Google maps, the *My Places* link was used to get to the maps developed by this account. The *Create new map* link was used to start developing the Irving CIKR map. The title of the map was added, a description of the map was added, and the unlisted box was marked to keep the maps web address from being listed in search engine results or other user profiles. The map was then saved.

An internet search of Irving Independent School District schools was conducted and resulted in a listing of all of the schools on the school districts web site. The address of each school was entered in the search bar on the Irving CIKR Google map. The map would find the school and put a temporary placemark on the map where the school was located. The Google map aerial photograph would be right clicked; *Add a placemark* would be selected from the options box; the name of the school would be placed in the title box; the address, phone number, and web site address of the school would be placed in the description box; the placemark icon would be left clicked and the green school house icon would be selected; OK would be selected and when the information box closed, the icon would be moved directly over the school building. This procedure was repeated for all of the schools in the Irving Independent School District. This procedure was also repeated for all of the City of Irving Fire Department and Police Department facilities.

Map Icons

It was realized that the default icons available on Google maps were not sufficient to delineate the vast array of CIKR that is found in the city. At this point, an internet

search for additional icons was conducted and two web sites with free icons were found. The most beneficial site was the google-maps-icons web site where the map-icon-collection 2.0 zip file was downloaded and used extensively. This collection of map icons contained 1301 individual icons (mollet, 2010). The other site that yielded a useful array of icons was IconArchive. This site contained an incredibly diverse set of 264,210 icons in 1391 icon sets (IconArchive.com, 2011). However, many of these icons were not suited for the purpose of mapping. The standardization of the google-map-icons made it the most useful icon set found and icons from the IconArchive were only used for marking private high schools and chemical sector facilities.

As CIKR locations were added to the map, the map became cluttered with icons unless it was zoomed in close enough to differentiate the locations that the icons were pinpointing. There were no controls to turn individual locations on or off, there was no functionality to organize individual locations into layers, and there was no functionality to add individual locations to a previously full page of CIKR locations. While researching these limitations on the internet in Google map user groups it was discovered that all of these limitations could be overcome by importing the Irving CIKR Google map into Google Earth.

Google Earth

Google Earth is a virtual globe that uses satellite imagery to provide a high resolution bird's eye view of the earth. Google Earth 6 can be downloaded for free at http://www.google.com/intl/en/earth (Google, 2011). To import a Google map to Google Earth, click the *View in Google Earth* hyperlink at the top of the Google Map. The

Google Map with all of its individual locations will open in Google Earth and will be located at the bottom of the *Places* window in the *Temporary Places* folder.

Building the Database

Once the database was established, it was decided to arrange the individual CIKR locations into to the 18 CIKR sectors defined by the NIPP. To accomplish this, the *My Places* label in the Places window was right clicked; the curser was placed over the *Add* option and the *Folder* option was selected. The folder was named for the Agriculture and Food Sector, the check box to *Allow this folder to be expanded* was checked, and the check box to *Show contents as options (radio button selection)* was left unchecked. This process was repeated for all 18 CIKR sectors.

With folders in the Places window representing all of the CIKR sectors defined in the NIPP, the individual CIKR locations from the Google Map were sorted into the appropriate sector specific folder. Where appropriate, sub-folders were added to the sector specific folders to provide layers of information that could be displayed on the map or removed from the map with a single mouse click. For example, the Transportation Systems Sector folder was sub-divided into folders for Air, Bus, Highways, Rail, and Pipelines. The Rail folder was then sub-divided into Freight and Passenger folders. One additional Boundary Lines folder was added to the 18 CIKR sector folders to contain the boundary lines for Dallas County, the City of Irving, and D/FW Airport.

Saving the Data

Once all of the CIKR locations were sorted into the appropriate sector folders and sub-folders, the temporary places folder was empty. To save the *My Places* folder in Google Earth, the *File* menu was left clicked, the curser was moved over the *Save* option,

and the *Save My Places* option was left clicked. Selecting this option saves the My Places folder allowing all of the locations in the My Places folder to be available the next time Google Earth is opened. After saving the My Places folder, the same procedure was followed that was used to save My Places to Google Earth with the exception of the final step. Instead of selecting the Save My Places option, The *Save Places As* option was selected and all of the data in the My Places folder was saved on the computer hard drive as a Google Earth .KML file.

Searching for CIKR

The search for CIKR locations in the City of Irving began with a review of Quick Action Plans (QAPs) that had been completed by fire department officers throughout the city. The CIKR information contained in these QAPs included the physical location of the buildings, the nature or business of the CIKR site, a sketch of the building footprint, contact information for the CIKR site, standpipe and sprinkler connection locations, Knox box locations, special hazards at the CIKR site, available water at the CIKR site, and a determination of the needed fire flow in GPMs. These QAP's were essentially pre-fire plans that were completed in the late 1990's and early 2000's with the most recent being dated in 2005. QAPs are stored in three ring binders in the captain's office at the fire stations and proved to be a valuable resource in identifying CIKR locations throughout the city.

On February 5, 2011, the Emergency Management Coordinator for the City of Irving, Pat McMacken, was approached about providing CIKR locations within the city for this applied research project. While quite forthcoming with information for fire department use, he was reticent about local CIKR information being published for public

consumption. He acknowledged that most of the information was available to the public from other outlets and that most of the information that was used by his office could be found on the internet. His office was willing to provide a digital copy of a CIKR map with the locations of schools, government facilities, and boundary lines of Dallas County, the City of Irving, and D/FW Airport (P. McMacken, personal communication, February 5, 2011).

The internet provided a vast array of resources to locate CIKR sites within the City of Irving. Water bodies, highways, railroads, pipelines, electricity power plants, electricity transmission lines and substations, stadiums, schools, police stations, monuments, malls, hospitals, fire stations, convention centers, and airports are all easily identified using Google Earth.

Natural gas and refined petroleum pipeline locations were found on the Texas Railroad Commission Public GIS Map Viewer (Texas Railroad Commission, 2011). Public safety locations, the Irving Convention Center, Irving City Hall, and other local government facilities were easily located by accessing the City of Irving web site (City of Irving, 2011). The Irving Independent School District web site provided the locations of all of their facilities along with contact information and web site addresses for each of their schools and administrative facilities (Irving Independent School District, 2011). This site also provided information on private schools, charter schools, colleges and universities, as well as information on Coppell Independent School District and Carrollton/Farmers Branch Independent School District schools, located within the City of Irving (Irving Independent School District, 2011). Once colleges, universities, and resorts were identified, their respective web sites provided campus maps that identified

individual buildings, recreation facilities, dorms, villas, sports fields, and other features on their property. The Google and Yahoo search engines were used to search for banking and finance locations, faith based locations, hotels and resorts, retail locations, senior living centers, sports and recreation locations, hospitals, urgent care locations, veterinarians, postal and shipping locations, bus terminals, and railroad terminals.

The TXU Northlake power plant, electric substations, and transmission lines were located by looking at the map on Google Earth, zooming in, and following the power lines. The power plant and each of the substations are identified by signage or placarding at their physical locations.

Terminal locations, parking locations, and public safety locations at D/FW Airport were identified using the interactive map on the D/WF Airport web site (Dallas/Fort Worth International Airport, 2011). Runway identification was made by using the Google Earth map, zooming in on the ends of each runway, and looking at the runway markings.

Nine of the Chemical Sector locations were identified from an email sent to all members of the Irving Fire Department by Assistant Fire Chief Victor Conley regarding *HazMat Responses to Structure Fires* (V. Conley, personal communication, August 27, 2010).

Making the Data Available by Request

As stated by DHS Office of Infrastructure Protection (2008):

> Effective CIKR information sharing relies on the balance between making information available to the appropriate authorities at all levels of government and the ability to protect sensitive or proprietary information, the disclosure of which might compromise ongoing law enforcement,

> intelligence, or military operations or methods. Dissemination of that information is therefore based on an end user's homeland security responsibilities and "need to know" the information in question (p. 4).

In accordance with this suggested DHS information sharing policy, and at the request of the City of Irving Office of Emergency Management, permission was requested, and granted, by the National Fire Academy to not publish the 771 CIKR sites collected and mapped as part of this applied research project in the appendix (see Appendix B). Instead, the data has been made available by request.

To gain access to this data, please send an email request to sjohnson@cityofirving.org and include your name, the organization that you are a part of, your position in that organization, and a statement about why you have a "need to know" this information. After reviewing your request, you will receive instructions for retrieving the Irving CIKR data file or you will receive a reply requesting more information about your need to access the Irving CIKR data file.

ACAMS, iCAV, and DHS Earth

After completing the CIKR database and the CIKR map for the City of Irving, it was discovered that the DHS had developed a similar suite of tools called ACAMS, iCAV, and DHS Earth. All of these tools are accessed through the use of a username and password on the HSIN secure, web-based portal for information sharing and collaboration. Application was made for membership in the HSIN Emergency Management COI and this application was in the nominating and vetting process at the time of this writing.

Limitations

For Official Use Only (FOUO)

Research into CIKR identification and the physical locations of CIKR in the City of Irving led to a vast amount of information, most of which was deemed For Official Use Only (FOUO). These documents generally included the following warning statement on the cover or somewhere on first few pages:

> This document is For Official Use Only (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO Information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.
>
> At a minimum when unattended, this document is to be stored in a locked container such as a file cabinet, desk drawer, overhead compartment, credenza, or locked area offering sufficient protection against theft, compromise, inadvertent access and unauthorized disclosure. (This warning statement is from a document marked FOUO and could not be cited.)

This information, while valuable for CIKR protection, was not available for use in this applied research project because of its FOUO designation. Upon submission of this applied research project the FOUO documents can be used to enhance the City of Irving CIKR Database and any CIKR not included in the database can be added and the City of Irving CIKR Map can be updated to include the additional CIKR information.

Time

CIKR identification and information gathering is a time consuming process that is better accomplished with multiple personnel collecting, compiling, entering, plotting, and checking the data. The 771 CIKR locations identified and included in this applied research project are the work of one individual working within a six month window for completion. With the time constraints removed and additional manpower provided additional locations can be added to the database and the information provided for each of the identified locations can be exponentially enhanced.

Definition of Terms

Infrastructure Protection – Actions to deter the threat, mitigate vulnerabilities, of minimize the consequences associated with an attack or disaster (United States Government Accountability Office, 2010, p. 4).

Infrastructure Resiliency – The ability to resist, absorb, recover from, or successfully adapt to adversity or a change in conditions (United States Government Accountability Office, 2010, p. 4).

Local Critical Infrastructure – Systems and assets, whether physical or virtual, so vital to the City of Irving that their incapacity or destruction would have a debilitating impact on local security, local economic security, local public health or safety, or any combination of those matters (Definition developed for this applied research project)Local Key Resources – Publically or privately controlled resources essential to minimal operations of the local economy or local government, including individual targets whose destruction could create a local disaster (Definition developed for this applied research project).

National Critical Infrastructure – Systems and assets, whether physical or virtual, so vital to the United States that their incapacity or destruction would have a debilitating impact on national security, national economic security, national public health or safety, or any combination of those matters (United States Government Accountability Office, 2007, p. 1).

National Key Resources – Publically or privately controlled resources essential to minimal operations of the economy or government, including individual targets whose destruction would not endanger vital systems but could create a local disaster or profoundly damage the nation's morale or confidence (United States Government Accountability Office, 2007, p. 1).

Key to Acronyms

ACAMS – Automated Critical Incident Management System

CIKR – Critical Infrastructure and Key Resources

COI – Communities of Interest

COP – Common Operational Picture

DHS – Department of Homeland Security

EOC – Emergency Operations Center

FOUO – For Official Use Only

HSIN – Homeland Security Information Network

HSPD-7 – Homeland Security Presidential Directive – 7

iCAV – Integrated Common Analytical Viewer

NCIP R&D – National Critical Infrastructure Protection Research and Development

NIPP – National Infrastructure Protection Plan

NOAA – National Oceanic and Atmospheric Administration

PCII – Protected Critical Infrastructure Information

QAP – Quick Action Plan

SSA – Sector Specific Agency

SSP – Sector Specific Plan

Results

Defining Critical Infrastructure and Key Resources

To answer the first two research questions, what critical infrastructure exists in the City of Irving and what key resources exist in the City of Irving, the terms critical infrastructure and key resources needed to be defined. The definitions used were modified versions of the definitions found in United States Government Accountability Office documents relating to CIKR protection. The modifications made were adjustments to the language that removed the national scope of the definitions and reshaped them into locally applicable definitions.

Critical infrastructure was defined as: systems and assets, whether physical or virtual, so vital to the City of Irving that their incapacity or destruction would have a debilitating impact on local security, local economic security, local public health or safety, or any combination of these matters.

Key resources were defined as: publically or privately controlled resources essential to minimal operations of the local economy or local government, including individual targets whose destruction could create a local disaster.

These definitions were useful until an attempt was made to categorize each of the CIKR locations as either a critical infrastructure location or as a key resource location. At

this point, the lines blurred and a majority of the locations found could be placed in either, or both, categories depending on the situation at hand in our new all hazards environment. While both research questions were valid, dividing the results into separate categories was not possible and did not change the information obtained for the City of Irving CIKR database or alter the development of the City of Irving CIKR map in any way. Therefore, both research questions were combined and could be stated as: What critical infrastructure and key resources exist within the City of Irving?

What Critical Infrastructure and Key Resources Exist Within the City of Irving?

The DHS separates CIKR into 18 sectors and assigns sector specific federal agencies to oversee each of the sectors. To align with the NIPP, the City of Irving CIKR Database (see Appendix C) has been organized alphabetically into the 18 CIKR sectors as defined by the DHS. In addition to the 18 DHS CIKR sectors, an additional section for boundary lines was included to clearly define the boundaries for Dallas County, the City of Irving, and DFW International Airport.

What's in the Database?

A total of 771 individual CIKR locations were defined in the database. Each item represents a physical location within the City of Irving, or just outside of the city limits, that could have an adverse impact on the city if that location experienced a terrorist attack, natural disaster, or manmade disaster.

The introduction to the database identifies HSPD-7 as the document establishing United States policy for CIKR protection, includes the definition of a CIKR sector, defines Federal SSA's, and lists the CIKR sectors along with their assigned SSA's as defined in the NIPP.

The introduction is followed by a section containing three boundary lines relevant to CIKR in the City of Irving. These boundary lines include: Dallas County, The City of Irving, and DFW International Airport.

Following this section are sections with the 18 alphabetically arranged CIKR sectors defined by the DHS. No locations were found within the City of Irving for four of these CIKR sectors. 10 of the remaining 14 CIKR sectors include alphabetically arranged sub-folders to aid in organizing the data.

The 18 CIKR Sector Locations

The following is a summary of the locations identified in the City of Irving CIKR Database arranged alphabetically by CIKR Sectors.

The Agriculture and Food sector contains two locations. Both of these locations are in the sub-folder for Food locations.

The Banking and Finance sector contains 61 locations. 43 of these locations are in the sub-folder for Bank Locations, four of these locations are in the sub-folder for Credit Card Processing Locations, eight of these locations are in the sub-folder for Credit Union Locations, three of these locations are in the sub-folder for Holding Company Locations, and three of these locations are in the sub-folder for Mortgage Company Locations.

The Chemical sector contains 10 locations. There are currently no sub-folders in this sector.

The Commercial Facilities sector contains 267 locations arranged into 6 sub-folders. 118 of these locations are in the Faith Based Locations sub-folder. This sub-folder is further broken down into sub-folders for Bah A'i Faith, Buddhist, Christian/Catholic/Evangelical, Hindu, Islamic, Jehovah's Witness, Jewish, LDS,

Satsang, Scientology, Sikh, and Universal. 107 of these locations are in the Hotel and Resorts Locations sub-folder. This sub-folder is further broken down into sub-folders for Country Clubs, Hotels, and Resorts. 10 of these locations are in the Private Sector Locations sub-folder. 19 of these locations are in the Retail Locations sub-folder. Nine of these locations are in the Senior Living Center Locations sub-folder and five of these locations are in the Sports and Recreation Locations sub-folder.

The Communications sector contains three locations. There are currently no sub-folders in this sector.

There are currently no CIKR locations in the Critical Manufacturing sector, Dams sector, or the Defense Industrial Base sector.

The Emergency Services sector contains 27 locations arranged into 4 sub-folders. 19 of these locations are in the City of Irving Locations sub-folder. This sub-folder is further broken down into sub-folders for Fire and EMS Locations and Police Locations. One of these locations is in the Dallas County Locations sub-folder. 6 of these locations are in the DFW International Airport Locations sub-folder. This sub-folder is further broken down into sub-folders for Fire and EMS Locations and Police Locations. One of these locations is in the Northlake College Locations sub-folder. This sub-folder is further broken down into a sub-folder for Police Locations.

The Energy sector contains 55 locations arranged into three sub-folders. 43 of these locations are in the Electricity Locations sub-folder. Two of these locations are in the Natural Gas Locations sub-folder. 10 of these locations are in the Refined Petroleum Locations sub-folder. This sub-folder is further broken down into sub-folders for Bulk Terminal Locations and Pipeline Locations.

The Government Facilities sector contains 207 locations arranged into five sub-folders. 76 of these locations are in the City of Irving Locations sub-folder. This sub-folder is further broken down into sub-folders for General Government Locations, Libraries, Parks, Pools, and Recreation Centers. One of these locations is in the Dallas County Locations sub-folder. 128 of these locations are in the Education Facilities sub-folder. This sub-folder is further broken down into sub-folders for Irving Independent School District, Carrollton/Farmers Branch Independent School District, Coppell Independent School District, Private Schools, and Colleges and Universities. One of these locations is in the Federal Government Facilities sub-folder and one of these locations is in the State Government Facilities sub-folder.

The Healthcare and Public Health sector contains 23 locations arranged into four sub-folders. One of these locations is in the CDC Stockpile sub-folder. Three of these locations are in the Hospitals sub-folder. Six of these locations are in the Urgent Care sub-folder and 13 of these locations are in the Veterinarians sub-folder.

The Information Technology sector contains three locations. There are currently no sub-folders in this sector.

The National Monuments and Icons sector contains one location. There are currently no sub-folders in this sector.

There are currently no CIKR locations in the Nuclear Reactors, Materials, and Waste sector.

The Postal and Shipping sector contains 28 locations arranged into four sub-folders. Six of these locations are in the FedEx sub-folder. Four of these locations are in the

United Parcel Service (UPS) sub-folder. Six of these locations are in the United States Post Office sub-folder and 12 of these locations are in the Trucking - Freight sub-folder.

The Transportation Systems sector contains 61 locations arranged into four sub-folders. 32 of these locations are in the Air sub-folder. Three of these locations are in the Bus sub-folder. 11 of these locations are in the Highway sub-folder and 15 of these locations are in the Rail sub-folder.

The Water sector contains 20 locations arranged into two sub-folders. 12 of these locations are in the Water Utilities sub-folder and eight of these locations are in the Waterways sub-folder.

Where are the CIKR Located Within the City of Irving?

The final research question resulted in a Google Earth™ City of Irving CIKR Map (see Appendix D) containing all 771 individual CIKR locations identified in the City of Irving CIKR Database.

The introduction to the database is contained in the Irving CIKR folder at the top of the folder list. The introduction identifies HSPD-7 as the document establishing United States policy for CIKR protection, includes the definition of a CIKR sector, defines Federal SSA's, and lists the CIKR sectors along with their assigned SSA's as defined in the NIPP.

The Irving CIKR folder is followed by a folder containing three boundary lines relevant to CIKR in the City of Irving. These boundary lines include: Dallas County, The City of Irving, and DFW International Airport.

Following this folder are folders with the 18 alphabetically arranged CIKR sectors defined by the DHS. No locations were found within the City of Irving for four of these

CIKR sectors. 10 of the remaining 14 CIKR sectors include alphabetically arranged sub-folders to aid in organizing the data. The data in these folders matches the data found in the City of Irving CIKR Database.

Discussion

City of Irving CIKR Database

The effort to build a CIKR database for the City of Irving started with a set of established QAP's that had not been updated in the last six to eight years. These QAP's provided a spring board that led to an explosion of data. Most of the information for the QAP's was collected by fire companies who physically visited each of the sites and walked through all of their facilities. This process was very manpower intensive and resulted in only slightly more information than could be garnered from an internet search coupled with aerial images of the facilities from any internet mapping web site.

It became obvious that the original intent of the QAP's, while not specifically stated, was to "identify, prioritize, and coordinate the protection of critical infrastructure and key resources" and to "prevent, deter, and mitigate the effects of deliberate efforts to destroy, incapacitate, or exploit them" (Bush, 2003). Only after stating these goals in HSPD-7 did President Bush put words to what the fire service had instinctively been doing for many years.

Initial efforts to identify CIKR were not organized and quite haphazard. However, finding the CIKR sites became much easier once they were broken down into the 18 critical infrastructure sectors defined in the NIPP. Instead of contemplating what sites may have some importance to the physical and economic security of the city and the region, the questions turned to what CIKR exists in the City of Irving that fits into the

Agriculture and Food Sector? What CIKR exists in the City of Irving that fits into the Banking and Finance Sector? What CIKR exists in the City of Irving that fits into the Chemical Sector? These questions continued for all 18 of the CIKR sectors defined in the NIPP. The answers to these questions led to an extensive database of CIKR locations within the City of Irving and a few that physically reside just outside of the city limits.

City of Irving CIKR Map

Mapping all of these locations also proved to be a challenge. Readily available mapping applications provided by the major search engines did not have adequate features for identifying similar CIKR sites or for layering these sites on the map so that sites, or groups of sites, could be turned on or off by the user. These internet based maps were also challenged by the quantity of information that they were populated with and did not provide a functionality to maintain the database of locations within the mapping application. These obstacles were overcome by moving the data to the more advanced Google Earth™ mapping application. With this mapping application the data could be organized into the 18 CIKR sectors defined in the NIPP; the individual sites, or entire layers, could be turned on or off to make the information more meaningful and/or less cluttered; and it was based on the Keyhole Markup Language (KML) making it easily distributable and capable of functioning in multiple mapping applications.

DHS Earth

The efficacy of using the Google Earth™ application was confirmed by the discovery of DHS Earth which is available through the HSIN. This secure, web-based CIKR data feed provides information in KML format; organizes the data into the 18 CIKR sectors defined in the NIPP; and opens using Google Earth™ or Microsoft Virtual

Earth. The data available in DHS Earth that is not contained within the City of Irving CIKR database includes worldwide population data, real-time situational awareness data, and weather related information. Other than these differences noted from the DHS description of this mapping application, this mapping tool was not available for further comparison until the HISN Emergency Management COI application process has been completed.

Interpreting the Results

While there may never be a complete CIKR database for any city, the 771 CIKR locations recognized in this applied research project are a good foundation for CIKR identification in the City of Irving. Visualizing these locations on Google Earth™ provides instant iconic information to the incident commander in the field and aids his ability to quickly become situationally aware; share a common operational picture with other decision makers on, or away from, the incident scene; make operational decisions based on other CIKR locations geographically adjacent to the incident scene; and plan additional operational periods based on the projected progression, or regression, of the incident.

The decision to use Google Earth™ for the City of Irving CIKR map was affirmed by the discovery of DHS Earth which is built using the same platform and programming language as Google Earth™.

Organizational Implications

The use of this CIKR database and CIKR map will improve Irving Fire Department emergency incident outcomes by providing the tools necessary to forecast the effects of cascading events and give incident commanders the information necessary to implement

appropriate countermeasures to protect against adverse effects or to mitigate the results of adverse effects that cannot be prevented. The City of Irving CIKR Database and the City of Irving CIKR Map, when used together, provide a powerful tabulated and graphical visualization for decision making that is free from any restrictions placed on it by any other governmental entity or private sector institution.

Recommendations

Based on extensive literature review, development of a 771 item database of CIKR in the City of Irving, and a fully functional City of Irving CIKR map, the City of Irving Fire Department is aligned with the recommendations of the NIPP in regard to CIKR protection planning within the City of Irving. However, the identification and protection of CIKR within the city is an ongoing venture that is constantly evolving and requires ongoing efforts to maintain an accurate database and visualization tool. To that end, the following recommendations are being made.

First, additional efforts should be made to improve the information contained within the database. The names and contact information of emergency contact personnel for each CIKR site should be acquired and updated on a regular basis. Digital floor plans should be included in the database that identify fixed systems within each of the CIKR sites. Systems such as sprinklers, standpipes, electrical breakers, gas valves, water valves, fire control rooms, elevator control rooms, as well as instructions for operating these systems should all be included in the database. Digital images of the CIKR sites and the systems they contain should also be compiled within the database.

Second, familiarization and training on the use of the CIKR database and CIKR map should be provided to all potential incident commanders. These digital tools are

quite user friendly but may not be seen as significant in the eyes of incident commanders that have never been exposed to technology. Basic computer usage skills are also required for these tools to be used effectively and skills training should be provided to any potential technology users who lack these skills.

Third, training scenarios should include the use of this technology to enhance familiarization of the new tools available in the incident command tool box.

Fourth, security should be maintained on all local CIKR information. This may mean loading the information onto password protected computers or making it available through a password protected network.

Fifth, public safety and emergency management department heads should evaluate the usefulness of HSIN, DHS COP, ACAMS, iCAV, and DHS Earth for their departments. The nomination and vetting process is quite slow and deliberate but could pay a large dividend with a wealth of information becoming available at no cost to their ever shrinking budgets.

Finally, it is highly recommended for future readers wishing to replicate this applied research project for their own jurisdiction to organize their database based on the CIKR Sectors defined in the NIPP. Once the CIKR Sectors are defined and the CIKR has been identified, it would be prudent to use the mapping technology currently in use by the DHS to develop your CIKR Map. All of the functions available in the DHS application will most likely not be available in commercially available applications but the freedom to use the information that is available will not be restricted by any entities other than your own.

References

Bush, G. W. (2003, December 17). *Laws and regulations.* Retrieved February 2011, 2011, from Homeland Security: http://www.dhs.gov/xabout/laws/gc_1214597989952.shtm#1

City of Irving. (2011). *Departments*. Retrieved February 26, 2011, from City of Irving, TX Official Site: http://www.ci.irving.tx.us/

Dallas/Fort Worth International Airport. (2011). *Interactive map*. Retrieved May 12, 2011, from Dallas/Fort Worth International Airport: http://www.dfwairport.com/imap/index.html

Google. (2011). *About google maps*. Retrieved February 12, 2011, from Google Maps: http://maps.google.com/support/bin/answer.py?hl=en&answer=7060

Google. (2011). *Google earth - Home*. Retrieved March 16, 2011, from Google Earth: http://www.google.com/intl/en/earth

IconArchive.com. (2011). *IconArchive beta*. Retrieved March 14, 2011, from iconarchive.com: http://www.iconarchive.com/

Irving Independent School District. (2011). *Other schools in Irving, TX*. Retrieved March 14, 2011, from Irving Independent School District: http://www.irvingisd.net/schools/city.htm

Irving Independent School District. (2011). *Schools*. Retrieved March 14, 2011, from Irving Independent School District: http://www.irvingisd.net/schools/default.htm

Knabb, R. D., Brown, D. P., & Rhome, J. R. (2006). *Tropical Cyclone report - Hurricane rita - 18 to 26 september 2005.* Miami, Florida: National Oceanic and Atmospheric Administration.

Knabb, R. D., Rhome, J. R., & Brown, D. P. (2006). *Tropical cyclone report - Hurricane katrina - 23 to 30 august 2005.* Miami, Florida: National Oceanic and Atmospheric Administration.

McNeill, J. B., & Weitz, R. (2010). *How to fix critical infrastructure protection plans: a guide for congress.* Washington, D.C.: The Heritage Foundation.

mollet, n. (2010, January 2010). *Map-Icons-Collection-2.0*. Retrieved March 14, 2011, from google-maps-icons: http://code.google.com/p/google-maps-icons/downloads/detail?name=map-icons-collection-2.0.zip

National Infrastructure Advisory Council. (2009). *Critical infrastructure resilience final report and recommendations.* Washington, D.C.: United States Department of Homeland Security.

National Oceanic and Atmospheric Administration. (2006, April 13). *NOAA reviews record setting 2005 atlantic hurricane season.* Retrieved February 14, 2011, from NOAA News: http://www.noaanews.noaa.gov/stories2005/s2540.htm

Office of Infrastructure Protection. (2008). *A guide to critical infrastructure and key resource protection at the state, regional, local, tribal, and territorial level.* Washington, D.C.: United States Office of Homeland Security.

Phillips, T. (2007, May 31). *Homeland security information network (HSIN).* Retrieved July 2, 2011, from DisasterHelp.gov: http://www.disasterhelp.gov/disastermanagement/library/archive/070606HSIN.ppt

Texas Railroad Commission. (2011). *RRC public map viewer*. Retrieved March 14, 2011, from Railroad Commission of Texas: http://gis2.rrc.state.tx.us/public/startit.htm

The 9/11 Commission. (2004). *The 9/11 commission report.* Washington, D.C.: The Government Printing Office.

The Department of Homeland Security Science and Technology Directorate. (2005). *The national plan for research and development in support of critical infrastructure protection.* Washington, D.C.: The Department of Homeland Security.

United States Department of Homeland Security. (2009, October 26). *Automated critical asset management system (ACAMS).* Retrieved July 2, 2011, from United States Department of Homeland Security: http://www.dhs.gov/files/programs/gc_1190729724456.shtm

United States Department of Homeland Security. (2010, June 28). *Integrated common analytical viewer (iCAV).* Retrieved July 2, 2011, from United States Department of Homeland Security: http://www.dhs.gov/files/programs/gc_1217445858859.shtm

United States Department of Homeland Security. (2011, April 28). *Homeland security information network.* Retrieved July 2, 2011, from United States Department of Homeland Security: http://www.dhs.gov/files/programs/gc_1156888108137.shtm

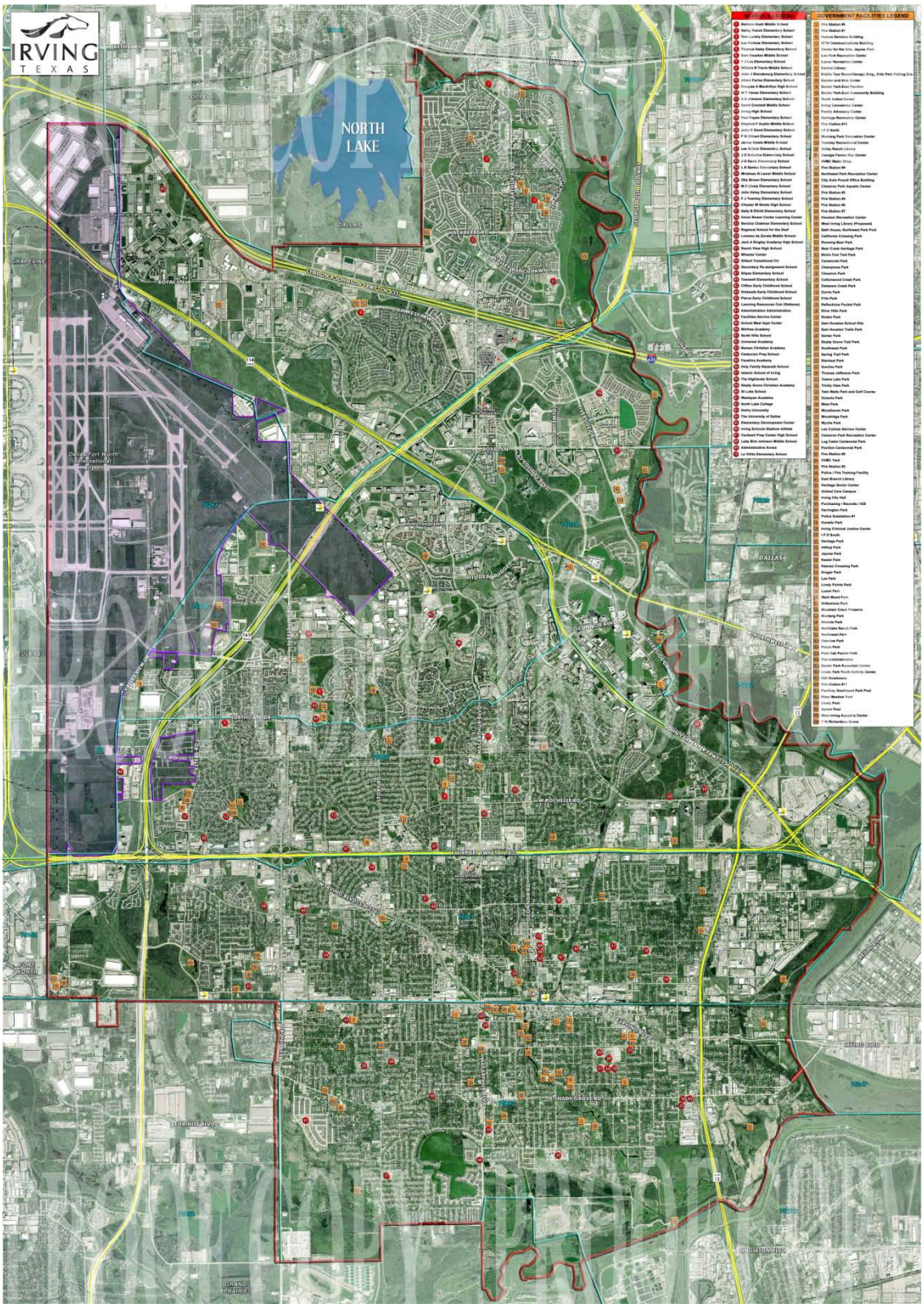
United States Government Accountability Office. (2006). *Critical infrastructure protection - progress coordinating government and private sector efforts varies by sectors' characteristics.* Washington, D.C.: U.S. Government Accountability Office.

United States Government Accountability Office. (2007). *Critical infrastructure protection: Sector plans and sector councils continue to evolve.* Washington, D.C.: United States Government Accountability Office.

United States Government Accountability Office. (2010). *Critical infrastructure protection - update to national infrastructure protection plan includes increased emphasis on risk management and resilience.* Washington, D.C.: United States Government Accountability Office.

Appendices

Appendix A – City of Irving, Department of Emergency Management CIKR Map



Appendix B – Permission to Not Publish the City of Irving CIKR Database

From: Burkell, Chuck [mailto:Chuck.Burkell@dhs.gov]
Sent: Thursday, July 07, 2011 2:34 PM
To: Scott Johnson
Subject: RE: EAFSOEM ARP

Scott,

You have my permission.

What I would suggest is to print this page and include it as an appendix item in your ARP. You can then refer the reader to it when/where necessary.

Hope this helps. Keep up the good work.

Sincerely,

Chuck Burkell

Executive Education Programs
U.S. Fire Administration/National Fire Academy
FEMA/Department of Homeland Security
16825 South Seton Avenue, Emmitsburg, Maryland 21727
(301) 447-1072 - - (301) 447-1178 (facsimile) chuck.burkell@dhs.gov

From: Scott Johnson [mailto:Fireboss7515@verizon.net]
Sent: Monday, June 27, 2011 5:16 PM
To: Burkell, Chuck
Subject: EAFSOEM ARP

Mr. Chuck Burkell,

My ARP for EAFSOEM is doing action research to develop a CIKR database and map for the City of Irving, TX.

I have created a database of 760 CIKR locations in the city.
I have also created a digital CIKR map using Google Earth so that the map would be portable and easily disseminated.

As I did my research I learned that DHS advises that:

“Effective CIKR information sharing relies on the balance between making information available to the appropriate authorities at all levels of government and the ability to protect sensitive or proprietary information, the disclosure of which might compromise ongoing law enforcement, intelligence, or military operations or methods. Dissemination of that information is therefore based on an end user’s homeland security responsibilities and “need to know” the information in question.”

The Emergency Management Coordinator for the City of Irving also has reservations about publishing the data for general consumption.

I would like permission to NOT include the research data in the appendix of my ARP.

Instead, I would like to make the data available on a request basis using a Windows Live™ SkyDrive account.
This would secure the data from being published in the LRC, and ultimately on the internet, but still make it available to my evaluator and any others with a legitimate "need to know".
In the **Results** section of my paper I would like to explain the need to secure the data and provide an email address for others to request the data.

If you would like, I would be happy to make the SkyDrive account available to you so that you can check it's functionality.

Thank you for your consideration,

Scott Johnson, Captain
Irving Fire Department
972-979-2750
Irving, Texas

Appendix C – Making the City of Irving CIKR Database Available by Request

As stated by DHS Office of Infrastructure Protection (2008):

> Effective CIKR information sharing relies on the balance between making information available to the appropriate authorities at all levels of government and the ability to protect sensitive or proprietary information, the disclosure of which might compromise ongoing law enforcement, intelligence, or military operations or methods. Dissemination of that information is therefore based on an end user's homeland security responsibilities and "need to know" the information in question (p. 4).

In accordance with this suggested DHS information sharing policy, and at the request of the City of Irving Office of Emergency Management, the 771 CIKR sites collected and mapped as part of this applied research project have not been published with this document. Instead, the data has been made available by request.

To gain access to this database, please send an email request to sjohnson@cityofirving.org and include your name, the organization that you are a part of, your position in that organization, and a statement about why you have a "need to know" this information.

After reviewing your request, you will receive instructions for retrieving the City of Irving CIKR Database file or you will receive a reply requesting more information about your need to access the information.

Appendix D – Making the City of Irving CIKR Map Available by Request

As stated by DHS Office of Infrastructure Protection (2008):

> Effective CIKR information sharing relies on the balance between making information available to the appropriate authorities at all levels of government and the ability to protect sensitive or proprietary information, the disclosure of which might compromise ongoing law enforcement, intelligence, or military operations or methods. Dissemination of that information is therefore based on an end user's homeland security responsibilities and "need to know" the information in question (p. 4).

In accordance with this suggested DHS information sharing policy, and at the request of the City of Irving Office of Emergency Management, the 771 CIKR sites collected and mapped as part of this applied research project have not been published with this document. Instead, the map has been made available by request.

To gain access to this map, please send an email request to sjohnson@cityofirving.org and include your name, the organization that you are a part of, your position in that organization, and a statement about why you have a "need to know" this information.

After reviewing your request, you will receive instructions for retrieving the City of Irving CIKR Map or you will receive a reply requesting more information about your need to access the information.